J.W. Price, 949/261-5433
Noboru Kattaelal
S.N. 09/593,677

OIPE JC1126
OCT 0 6 2000
PATENT & TRADEMARK OFFICE

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

NAK1-BL38

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　６月１５日

出願番号
Application Number: 平成１１年特許願第１６７８９９号

出願人
Applicant (s): 松下電器産業株式会社

２０００年　６月　２日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０４１２２４

【書類名】　特許願

【整理番号】　2022510291

【提出日】　平成11年 6月15日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　勝田　昇

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　茨木　晋

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　井上　信治

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　暗号処理装置および暗号復号装置および暗号伝送方法および記録装置およびデータ書き込み装置

【特許請求の範囲】

【請求項１】暗号処理手段と複数の入力データ解析手段と前記入力データ読み取り手段を制御し暗号処理位置を検出して暗号処理手段に暗号処理させる制御手段を具備し、前記制御手段は、暗号処理手順を記述した暗号処理記述データを読み取り、前記暗号処理記述データに基づき暗号処理制御を行うことを特徴とする暗号処理装置。

【請求項２】暗号化処理記述データは、専用に定義された入力データ解析処理の組み合わせによる処理手順を含み、入力データ解析装置は、前記専用に定義された入力解析処理を行うことを特徴とする請求項1記載の暗号処理装置。

【請求項３】入力データ解析手段としてデータ中のデータヘッダー位置を検出するヘッダー検出手段を少なくとも具備することを特徴とする請求項１記載の暗号処理装置。

【請求項４】入力データ解析手段としてデータ中の読み取り基本単位のデータ長を検出するデータ長検出手段を少なくとも具備することを特徴とする請求項1記載の暗号化装置。

【請求項５】暗号復号処理手段と複数の入力データ解析手段と前記入力データ読み取り手段を制御し暗号処理位置を検出して暗号処理手段に暗号処理させる制御手段を具備し、前記制御手段は、暗号処理手順を記述した暗号処理記述データを読み取り、前記暗号処理記述データに基づき暗号復号処理制御を行うことを特徴とする暗号復号処理装置。

【請求項６】暗号化処理記述データは、専用に定義された入力データ解析処理の組み合わせによる処理手順を含み、入力データ解析装置は、前記専用に定義された入力解析処理を行うことを特徴とする請求項第６項記載の暗号復号処理装置。

【請求項７】入力データ解析手段としてデータ中のデータヘッダー位置を検出するヘッダー検出手段を少なくとも具備するすることを特徴とする請求項５記載

の暗号復号装置。

【請求項８】入力データ解析手段としてデータ中の読み取り基本単位のデータ長を検出するデータ長検出手段を少なくとも具備することを特徴とする請求項５項記載の暗号復号装置。

【請求項９】伝送データを暗号化鍵と暗号処理記述データに基づき暗号化し、前記暗号化により暗号化された暗号化データと暗号化鍵および暗号処理記述データを伝送することを特徴とする暗号伝送方法。

【請求項１０】記録対象のデータを前記データに施される暗号処理内容を示す暗号処理記述データと前記暗号化処理記述データに基づき暗号化したデータを記録する記録装置。

【請求項１１】さらに、あらかじめ暗号処理記述データ記憶手段を持ち、データ記録時に前記記憶するデータを記録する際に適切な暗号処理記述データを送信することを特徴とする請求項１０記載の記録装置。

【請求項１２】暗号化処理手段、記録装置内の暗号処理記述データ読み出し手段を具備し、データ書き込み時に、記録装置にある暗号化記述データを読み出し、それに基づき書き込みデータを暗号化して記録装置に書き込むことを特徴とするデータ書き込み装置。

【請求項１３】暗号処理記述データ読み取り手段と暗号復号化手段を持ち、データ読み出し時、それに対応する暗号処理記述データを読み出し、前記暗号処理記述手段に基づき読み出しデータを暗号復号化処理することを特徴とするデータ読み出し装置。

【請求項１４】暗号処理手段と暗号復号処理手段を持ち、暗号復号手段は、暗号化されたデータの暗号処理記述データを読みとり、それに基づき暗号復号処理し、暗号処理手段は、所望の暗号化処理を記述した第2の暗号化処理記述データを読み込み、読み込んだ第2の暗号処理記述データに基づき暗号化処理することを特徴とする暗号変換装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データの伝送および蓄積においてデータを暗号化する暗号処理装置および暗号復号装置およびそれを用いた暗号伝送方法および暗号化処理して記録する記録装置およびデータ書き込み装置およびデータ読み出し装置および暗号変換装置に関するものである。

【０００２】

【従来の技術】

従来の暗号化処理は、データの伝送および蓄積等において許可のあるものだけがそれを利用できるようにするため用いられている。たとえば、テレビのディジタル放送においては、有料放送を行う際、番組データに暗号処理を施している。その際、暗号化処理するデータとしては、各伝送パケット内のデータのペイロード部分にのみ暗号化することが規定されている。したがって、送信側で規定された暗号アルゴリズムを用いて、規定された位置を暗号化する。一方、復号側は、規定された暗号復号アルゴリズムにより規定された領域を暗号復号処理すれば、元のデータを得る事が出来る。ここでの暗号復号アルゴリズムとは、たとえば、６４ビットのブロック暗号としてDES暗号やFEAL暗号などの共通鍵暗号アルゴリズムあるいは、公開鍵暗号のRSA暗号といったものを指す。

【０００３】

このように、従来の暗号装置では、暗号アルゴリズムを決定するのに加えて暗号処理する位置について正確に規定することで暗号化復号化処理をおこなっていた。

【０００４】

【発明が解決しようとする課題】

しかしながら、前記従来の暗号化処理では、暗号アルゴリズムに加えて、厳密にデータ中のどの領域を暗号化対象にするかを規定しているため、想定したデータ以外を暗号化復号化処理することが困難であった。

【０００５】

たとえば、映像や音楽データなどを暗号化して記録する場合、それぞれを再生する場合にランダムアクセスによる再生や早送り、途切れのない再生などを行うため、各データの記録フォーマットにある基本アクセス単位で暗号化処理を切り

換えることが望まれている。

【０００６】

また、すべてのデータをCBCモード（サイファーブロックチェーンモード）など最初のデータに依存して暗号化すると途中のデータをアクセスする場合も最初のデータから順に再生しなければならず不便である。

【０００７】

したがって、暗号化するデータのフォーマットに応じてランダムアクセスに必要な情報は残して暗号化するといった暗号化領域や処理の更新タイミング等をそれぞれのシステムに応じて規定する必要がある。ところが、DVD-RAMディスクやハードディスクおよび固体メモリーカードなど大容量のメモリなどさまざまなフォーマットの映像や音声を記録することが想定される機器においては、それらのデータのコンテンツに応じて別々の暗号処理装置が必要になる問題があった。

【０００８】

また、同一フォーマットであっても記録するメディアによってアクセス可能なデータ単位があり、記録メディアに依存したアクセス単位でアクセスが可能になるように暗号処理の更新位置を切り換える必要があるが、それぞれの記録メディア毎に暗号処理装置を用意することは、非常に効率が悪い問題があった。

【０００９】

また、伝送路についてもその伝送パケット長などに依存して暗号処理領域を決定することが多く、複数の伝走路から受信する場合を考えるとそれぞれについて専用の暗号装置を持つのは、非効率的である。

【００１０】

またに、ディジタルデータ、蓄積メディアおよび伝送路のフォーマットについても今後更に新しいものが出現されてくることが考えらる。したがって、単にビット列を解読困難にするように設計された暗号アルゴリズムを、暗号化するデータ中の所望の位置に適切に施して行える暗号装置が必要とされていた。

【００１１】

以上のような問題点を鑑み本発明は、データのフォーマット、記録されるメディアフォーマット、伝送路フォーマット等に応じた最適な暗号処理が特にそのフ

ォーマット専用に作り込むことなく行え、さらに今後出現するフォーマットについてもそれに適した暗号処理が可能な汎用的な暗号処理装置およびそれを用いた伝送方法および記録装置およびデータ書き込み装置およびデータ読み出し装置および暗号変換装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】

前記課題を解決するために本発明は、暗号処理手段と複数の入力データ解析手段と前記入力データ読み取り手段を制御し、暗号処理位置を検出して暗号処理手段に暗号処理させる制御手段を具備し、前記制御手段は、暗号処理手順を記述した暗号処理記述データを読み取り、前記暗号処理記述データに基づき暗号処理制御を行う構成であり、暗号処理記述データを入力することにより多様なデータフォーマットに大要可能な暗号処理装置とできる。

【００１３】

また、本発明は、暗号処理記述データは、専用に定義された入力データ解析処理の組み合わせによる処理手順を含み、入力データ解析装置は、前記専用に定義された入力解析処理を行うものであり、暗号記述が効率的に行える。

【００１４】

また、本発明は、入力データ解析手段としてデータ中のデータヘッダー位置を検出するヘッダー検出手段を少なくとも具備する構成である。

【００１５】

また、入力データ解析手段としてデータ中の読み取り基本単位のデータ長を検出するデータ長検出手段を少なくとも具備する構成である。

【００１６】

また、本発明は、暗号復号処理手段と複数の入力データ解析手段と前記入力データ読み取り手段を制御し、暗号処理位置を検出して暗号処理手段に暗号処理させる制御手段を具備し、前記制御手段は、暗号処理手順を記述した暗号処理記述データを読み取り、前記暗号処理記述データに基づき暗号復号処理制御を行う暗号復号処理装置の構成である。

【００１７】

また、暗号化処理記述データは、専用に定義された入力データ解析処理の組み合わせによる処理手順を含み、入力データ解析装置は、前記専用に定義された入力解析処理を行う暗号復号装置の構成である。

【００１８】

また、さらに本発明は、入力データ解析手段としてデータ中のデータヘッダー位置を検出するヘッダー検出手段を少なくとも具備する暗号復号装置の構成である。

【００１９】

また、さらに入力データ解析手段としてデータ中の読み取り基本単位のデータ長を検出するデータ長検出手段を少なくとも具備する暗号復号装置の構成である。

【００２０】

また、本発明は、伝送データを暗号化鍵と暗号処理記述データに基づき暗号化し、前記暗号化により暗号化された暗号化データと暗号化鍵および暗号処理記述データを伝送する暗号伝送方法である。

【００２１】

また、本発明は、記録対象のデータを前記データに施される暗号処理内容を示す暗号処理記述データと前記暗号化処理記述データに基づき暗号化したデータを記録する記録装置の構成である。

【００２２】

また、本発明は、あらかじめ暗号処理記述データ記憶手段を持ち、データ記録時に前記記憶するデータを記録する際に適切な暗号処理記述データを送信する記録装置の構成である。

【００２３】

また、本発明は、暗号化処理手段、記録装置内の暗号処理記述データ読み出し手段を具備し、データ書き込み時に、記録装置にある暗号化記述データを読み出し、それに基づき書き込みデータを暗号化して記録装置に書き込むデータ書き込み装置の構成である。

【００２４】

また、本発明は、暗号処理記述データ読み取り手段と暗号復号化手段を持ち、データ読み出し時、それに対応する暗号処理記述データを読み出し、前記暗号処理記述手段に基づき読み出しデータを暗号復号化処理するデータ読み出し装置の構成である。

【００２５】

また、本発明は、暗号処理手段と暗号復号処理手段を持ち、暗号復号手段は、暗号化されたデータの暗号処理記述データを読みとり、それに基づき暗号復号処理し、暗号処理手段は、所望の暗号化処理を記述した第2の暗号化処理記述データを読み込み、読み込んだ第2の暗号処理記述データに基づき暗号化処理する暗号変換装置の構成である。

【００２６】

【発明の実施の形態】

以下、本発明の実施の形態について図１から図１０を用いて説明する。

【００２７】

（実施の形態１）

図１は、本発明の第１の実施の形態における暗号処理装置の構成図である。同図において、１０１は、暗号処理装置、１０２は、制御部、１０３は、暗号処理部、１０４は、フレーム長検出部、１０５は、ヘッダー検出部である。以上の構成において以下その動作を説明する。

【００２８】

暗号処理装置１０１は、暗号化鍵と暗号処理記述情報に基づき入力データを暗号化処理する。暗号化鍵は、制御部１０２に入力されると暗号化処理部１０３に入力される。

【００２９】

暗号処理記述情報は、入力データ中のどの部分に暗号化するのかを示す情報、あるいは、どのようにその特定のデータ領域を見つけて暗号化処理するかという動作を表現した情報である。図２は、暗号処理記述情報を表現するために定義した処理命令関数の説明図である。同図において、４つの専用命令関数を定義している。図２（１）の関数は、ディジタルデータにおける読み出しの同期をとるこ

とが可能にするための同期信号パターンを検出するヘッダー検出関数である。これは、検出するヘッダーの検出パターンのビット数とそのパターンと検出開始位置を入力パラメータとして、入力データ中の検出開始位置から最初に検出される検出パターン位置へ参照位置を移動する処理であり、図１におけるヘッダー検出部１０５の処理を記述する。図２（２）は、同期パターンに囲まれた入力データのフレーム長を検出するフレーム長検出処理を示す関数である。これは、入力データが可変長である場合、よくそのフレーム長を示すコードが付加されている場合があり、それを検出する処理である。ヘッダーの先頭からそのコードが出現する位置のビット位置とそのコードの符号長、および表現されている値のの単位がバイト単位かビット単位かを示す値を引数として検出した値に単位ビット倍されて、符号長が検出され、frame#length値に値をいれる。これは、図１のフレーム長検出処理部１０４の処理を表現する。

【００３０】

図２（３）は、入力データ中の参照位置を引数分だけ移動させる処理である。

【００３１】

図２（４）は、暗号処理を示す関数で図１の暗号処理部１０３の処理を表現する。アルゴリズム番号は、ＤＥＳやＦＥＡＬといったあらかじめ標準で準備した暗号アルゴリズムである。モードは、暗号の適応モード、block#lengthは、処理ブロック長であり、たとえば、６４ビットのブロック暗号でＥＣＢモードであれば、６４ビットである。終了処理位置は、暗号処理する領域の最終ビット位置であり、もし暗号処理領域のビット数が処理ブロック長で割り切れなかったら終了処理位置を越えない最大の回数だけ処理するものとする。

【００３２】

図３は、図２で定義された関数を用いて記述された暗号処理記述情報の例の説明図である。同図で記述された処理は、同期ヘッダーパターンが１２ビットで１６進数表現でＦＦＦであり、ヘッダー先頭位置より３１ビットめから１３ビットにフレーム長コードがあるデータについてフレーム長コード以下をＤＥＳアルゴリズムでＣＢＣモードで処理することを記述したものである。このデータは、たとえば、ＭＰＥＧ２あるいはＭＰＥＧ４標準で規定されたオーディオデータのＡ

ＡＣで圧縮されたデータのフォーマットにある。このようなオーディオデータを再生する用途として、ランダムアクセス等を行いたい場合は、所望のフレーム位置に参照位置を移動して再生処理をおこなう必要があり、フレーム位置が検出しやすいように同期パターンを暗号化せずに残すとともに次のフレームの先頭を暗号化後でもわかるようにフレーム長コードも暗号化せずに残す方が便利である。

【００３３】

図３に戻って、最初のヘッダー位置は、データの先頭にあるとして、参照位置を０ビットめにし、その後ヘッダー位置を検出し、フレーム長コードを検出し、次に参照位置をフレーム長コード位置の直後に移動する。検出したフレーム長に基づき、暗号処理終了位置を算出した後、暗号処理を行う。その後、暗号処理終了位置に参照位置を移動して、再びヘッダ検出処理から繰り返すことでヘッダーおよびフレーム長コードを残した領域を暗号化処理する記述となる。

【００３４】

以上のように記述された情報をそのままテキスト形式でもよいし、あるいは、各関数命令および変数に適当な数値を割り当てることでデータ量の少ないバイトコードのプログラムとして暗号処理記述情報とする。以上のように記述された暗号記述情報が制御部１０２に入力される。

【００３５】

図１に戻って、制御部１０２は、暗号処理記述情報を解釈し、それに基づきヘッダー検出処理部１０５、フレーム長検出部１０４を制御し、暗号処理領域を検出するとともに、暗号処理タイミングになると暗号処理関数に示された処理に基づき暗号処理部１０３に暗号処理を行わせることにより暗号化データを得る。

【００３６】

以上のような動作により暗号処理装置１０１は、暗号処理記述情報に基づき所望の位置に暗号化処理できる。暗号処理記述情報は、図２のような命令関数のようにディジタルデータの多くのものに共通に存在するヘッダーやフレーム長コード検出命令を特別に持つことにより、簡潔な表現で大半のディジタルデータフォーマットについてヘッダー部分を残した部分への暗号化処理を記述できるし、もっと処理の簡単なフレーム単位に関係なく、一定長ごとに暗号処理することなど

多様な暗号処理を表現できる。

【００３７】

（実施の形態２）

図４は、本発明の第２の実施の形態である暗号復号装置の構成図である。同図において、４０１は、暗号処理装置、４０２は、制御部、４０３は、暗号復号処理部、４０４は、フレーム長検出部、４０５は、ヘッダー検出部である。以上の構成において以下その動作を説明する。

【００３８】

図４は、図１の暗号処理部１０３を暗号復号処理部４０３に置き換えたものである。

【００３９】

暗号処理された位置については、まったく同様の処理によって導き出される。したがって、図２の命令関数に加えてdecryption(algorithim#no, mode, blocklength, end#pnt)を図２の暗号処理を暗号復号処理に置き換えた形で定義してやれば、同様にその動作を記述できる。

【００４０】

たとえば、図３の暗号化処理は、encryption命令をdecryption命令に置き換えるだけで図２の記述に対する復号処理記述となる。したがって、あとは同様の処理により図１で暗号化されたデータは、復号処理される。

【００４１】

図５は、図１と図４の暗号処理装置１０１と暗号復号処理装置４０１を用いた暗号伝送装置の構成図である。同図において、５０１は、暗号処理記述情報、５０２は、図１の暗号処理装置１０１と同等の処理を行う暗号処理装置、５０３は、多重送信装置、５０４は、受信多重分離装置、５０５は、暗号処理記述言語５０１の暗号処理命令を暗号復号処理に置き換えた暗号処理記述情報、５０６は、図４の暗号復号処理装置４０１相当の暗号復号処理装置である。以上の構成により、以下その動作を説明する。

【００４２】

送信データは、暗号化処理装置５０２に入力される。暗号処理記述情報５０１

は、図３で示したような暗号処理動作を記述したものであり、送信データを送信するのに適切な暗号処理を行うように記述する。たとえば、CBCモードを用いた場合伝送途中でエラーが発生すると再生が困難になることを考慮して、フレーム毎に処理を初期化して行うことなどで伝送エラーに対する対策を取るなどが考えられる。図３の記述もフレーム毎のCBC処理を行うことを記述している。

【００４３】

図５に戻って、暗号処理装置は、暗号記述情報５０１と暗号化鍵Kを用いて送信データを暗号化処理して多重送信装置５０３に送られる。多重送信装置５０３は、暗号化された送信データに暗号化鍵Kと暗号処理記述情報５０１中の暗号処理命令部分を暗号復号処理命令に置き換えたものを多重して受信多重分離装置５０４へ伝送する。受信多重分離装置５０４は、暗号化鍵Kおよび暗号処理記述情報５０５を分離して暗号復号処理装置５０６に入力するとともに暗号化されてきたデータを暗号復号処理装置５０６へ入力する。暗号復号処理装置５０６は、暗号処理記述情報５０５に基づき、暗号復号処理することにより受信データを得る。以上のような動作により、暗号伝送装置自身は、送信するデータについて特別に作り込まれたものでなくても暗号処理記述情報により暗号化し、その暗号化処理情報を暗号化鍵とともに伝送することで送信データの特徴に応じて最適な暗号化処理を施して伝送できる。また、送信データの種類が１つではなく、映像情報やオーディオ情報など異なるフォーマットのデータが伝送される場合でも暗号処理記述情報を書き換えることで暗号処理装置を複数もつ必要がない。

【００４４】

（実施の形態３）

図６は、本発明の第3の実施の形態である暗号処理装置を用いたデータ書き込み読み出し装置およびデータ記憶装置の構成図である。同図において、６０１は、データ書き込み読み出し装置、６０２は、ディジタルスチルカメラやオーディオプレイヤーなどに利用されるメモリカードに代表されるようなデータ記憶装置、６０３は、制御部、６０４は、鍵生成部、６０５は、図１の暗号化処理装置の暗号処理部１０３に図４の暗号復号処理部４０３の機能をあわせて持たせた暗号／復号処理部、６０６は、データ記憶装置６０２屁の記憶するデータを格納した

り、データ記憶装置６０２からのデータ読み出し時にデータを格納する記録部、６０７は、制御部、６０８は、データ記憶装置６０２に記録される可能性があると想定されるいくつかのデータフォーマットに対してあらかじめ用意した暗号処理記述情報群を記録した暗号処理記述情報記憶部、６０９は、データ記憶装置６０２に与えられたメディアID番号記憶部、６１０は、データ記録部である。これは、近年、メモリーカードを用いたオーディオプレイヤーやカメラなどにおいて著作権の保護の対象となるデータのディジタル記録において複数のコピーが容易に作れない様に記録メディアのIDに依存したパラメータでデータを暗号化して記録することにより、著作権を守る処理を保証した製造者の装置だけが復号処理ができるようにすることで無数の複製を作られることを防止するためなどに用いることが出来る。以上のような構成について以下その動作を説明する。

【００４５】

データ書き込み読み出し装置６０１は、たとえば、ディジタルスチルカメラやオーディオプレーヤー内のメモリカードとのインターフェイス部であったり、パーソナルコンピュータとメモリカードを接続するインターフェイス部であったりするものであり、外部からの入力データをデータ記憶装置６０２に書き込んだり、逆に外部から指定によりデータ記憶装置６０２中のデータを読み出し出力することが想定される。ここでは、外部の入出力のかわりに記録部６０６からの書き込み、記録部６０６への読み出しにより説明する。

【００４６】

データ記憶装置６０２への書き込み読み出し、制御部６０３および６０７間のデータ転送手順により行われる。

【００４７】

図８は、データ書き込み時の制御部６０３と制御部６０７間の処理の説明図である。同図において、８０１は、書き込みファイル指定処理、８０２は、メディアIDおよび暗号処理記述情報送出処理、８０３は、暗号化鍵設定処理、８０４は、暗号処理記述情報設定処理、８０５は、暗号化およびデータ送出処理、８０６は、受信データ記録処理である。

【００４８】

図８における左側の処理は、制御部６０３の処理であり、右側の処理は、制御部６０７の処理である。まず、制御部６０３は、書き込むファイル名を制御部８０２に送出する。制御部８０７は、指定されたファイル名につけられた拡張子（たとえば、そのデータのフォーマットの略称名をファイルの拡張子としてあらかじめ定義しておいたもの）を用いて、暗号処理記述情報記憶部６０８から送られてくるデータに対応した暗号処理記述情報を読み出し、メディアID番号記憶部６０５内のメディアIDとともに制御部６０３へ伝送する。制御部６０３は、メディアIDを鍵生成部６０４へ送る。鍵生成部６０４は、あらかじめ決められた処理に基づき暗号化鍵を生成し、暗号／復号処理部６０６へ暗号化鍵を入力する。次に、制御部６０３は、暗号記述情報を暗号／復号処理部６０５へ設定する。そして、記録部中の該当ファイルを暗号化処理部６０５へ送出し、暗号処理後のファイルを制御部６０７へ送出する。制御部６０７は受信データを指定ファイル名で記録する。

【００４９】

図９は、データ読み出し時の制御部６０３および制御部６０７の処理フローの説明図である。同図において、９０１は、読み出しファイル名送出処理、９０２は、暗号処理記述情報およびメディアID送出処理、９０３は、暗号化鍵設定処理、９０４は、暗号記述情報設定処理、９０５は、データ送信リクエスト処理、９０６は、データ送信処理、９０７は、データ受信処理である。

【００５０】

図９における左側の処理は、制御部６０３の処理、右側は、制御部６０７の処理である。まず、制御部６０３はは、データ記憶装置６０２より読み出したファイル名を指定するためファイル名を制御部６０７へ送信する。制御部６０７は、指定ファイルの拡張子などの属性に基づいて、それに対応した暗号処理を復号するための暗号処理記述情報を選択し、メディアIDとともに制御部６０３に送信する。この時の暗号処理記述情報は、そのファイルが書き込まれた際の暗号処理記述情報の暗号処理命令部分を暗号復号処理命令に入れ替えたものと同じである。制御部６０３は、メディアIDを鍵生成部６０４へセットする。鍵生成ぶ６０４は、データが書き込まれた時と同じ鍵を生成することになり、その鍵が暗号／復号

処理部６０５に設定される。次に制御部６０３は、暗号処理記述情報を暗号処理部へ設定する。その後、ファイルデータの送信を制御部６０７へリクエストする。制御部６０７は、リクエストを受け取ると指定されたファイルデータを制御部６０３へ送出する。制御部６０３は、受信したファイルデータを暗号／復号処理部６０５で復号処理させて記録部６０６へ記録する。

【００５１】

以上の処理により、データ記憶装置６０２へは、そのデータフォーマットに適切な方法で暗号化処理され記録され、また、読み出し時には、正しく再生される。そして、データ書き込み読み出し装置６０１での処理手続きを踏まずに直接データにアクセスしてもデータは、データ記憶装置６０２のメディアIDに依存した暗号化されているため、複製を作って正しく再生することが出来ず、不正な複製を防止出来る。

【００５２】

図７は、データ記憶装置６０２内でのファイルの記録構成の説明図である。四角で囲まれたものがファイルとして管理されているものとする。データ記録装置６０２では、上段に示されたように各拡張子用にそれぞれ暗号処理記述情報が記憶されている。それは、最下段に示された各記録データファイルの拡張子によって関係づけて管理する。中段にある記録データファイルに対応した暗号鍵ファイルである。これは、先に説明した図８、図９の手続きでは、存在しない。先の説明では、データ記憶装置６０２のデータは、同じ鍵で暗号化されることになるため、たとえば、図７の中段のように各ファイルに対応した暗号化鍵ファイルを生成させることで各ファイルに独立の鍵を持たせることができる。これは、たとえば、図６の鍵生成部が適当に乱数を生成し、それをメディア鍵とともにもう一つの鍵生成パラメータとして暗号化鍵を生成し、その乱数をそのファイル用暗号化鍵として制御部６０３を通じてデータ記憶装置６０２に伝送して暗号化鍵ファイルとして記憶させ、読み出し時には、メディアIDを送出する時に同時に暗号鍵ファイルをおくこととして、鍵生成部にメディアIDと暗号鍵ファイルを与えることにより暗号化鍵を生成させる。そうすることでデータ記憶装置６０２内のデータは、メディアIDとそのファイルに対応した暗号化鍵ファイルデータに依存した鍵

で暗号化されていることになり、各データは、別々の暗号化鍵で暗号化処理された形となりより解読に対して安全な管理が行える。また、想定されるフォーマットに対する暗号化処理記述情報をそのフォーマット毎に用意しているのですべてのファイル毎に暗号化処理記述情報ファイル持つ必要がなく、保存データ量を少なく出来る。

【００５３】

図１０は、データを記録するメディアに適した暗号化処理に切り換える場合の暗号処理変換処理の説明図である。同図において１００１、１００２は、DVDやメモリカードなどの互いに異なる記録メディア、１００３は、記録メディア１００１のメディアID読み取り部、１００４は、記録メディア１００２のメディアID読み取り部、１００５は、制御部、１００６は、図２の暗号復号処理装置相当の暗号復号部、１００７は、図１の暗号処理装置相当の暗号処理部である。同図の構成において、以下で暗号変換処理を説明する。

【００５４】

データを読み出しする場合にそのランダムアクセス性に影響するものとして、記録メディアのデータアクセス単位がある。すなわち、それぞれのメディアにおいて一度にアクセスできる単位で記録データのランダムアクセス単位が決まる場合がある。その際、暗号化処理もそのアクセス単位にあわせて処理単位を決定し、暗号化処理するれば、再生時のランダムアクセス性を悪化させることがない様にできる。そこで、各メディアにそれぞれそのアクセス単位に適合した暗号処理記述情報を持たせ、すべての記憶データファイルは、この記述に基づき暗号化して保存させる。図１０は、記録メディア１００１から記録メディア１００２へデータを移し替える際の暗号変換処理を説明している。まずメディア鍵読み取り部１００３および１００４は、それぞれの記録メディア１００１、記録メディア１００２よりそれぞれのメディアIDを読み出してくる。制御部１００５は、メディア鍵を暗号復号部１００６、暗号処理部１００７にそれぞれが接続された暗号処理に対応させて設定する。記録メディア１００１では、各データは、記憶データの基本アクセス単位がたとえば512バイトなら、その単位で暗号化が行われるように記述した暗号化処理記述情報ファイルがあり、記録されているデータファイ

ルはこれに関係づけられている。ファイル送出時は、暗号処理記述情報を読み取り暗号復号処理部１００６に設定した後、転送するデータを暗号復号処理部１００６へ入力させる。記録メディア１００１の場合と同様に記録メディア１００２側にも記録メディアに適した暗号処理記述情報が用意されている。そして、データ受け入れ時は、制御部１００５が記録メディア１００２用の暗号処理記述情報を暗号処理部１００７に設定する。そして、暗号復号処理部１００６からの出力を暗号化処理部１００７が暗号処理することで、記録メディア１００２に適した暗号処理方法に変換された暗号化処理が施されて記録メディア１００２に記録される。以上のような処理により、それぞれの記録メディアに適した暗号処理記述を暗号変換部にそれぞれ与えて、暗号復号処理、暗号処理を行うことでそれぞれのメディア内でのデータのアクセス操作性を失わせることのない暗号変換処理が行える。

【００５５】

以上、説明したように、本発明の実施の形態では、ディジタルデータで一般に考えられるデータの同期ヘッダー検出およびフレーム長の検出といった処理を専用に規定した暗号記述言語に基づき暗号処理を記述した暗号処理記述情報と、専用に規定した処理を実現する処理部を具備し、それを制御する制御部が暗号処理記述情報を解釈して各処理を制御させる構成により、多様なディジタルフォーマットに対してその特性に応じた適切な暗号処理を行うことができる。

【００５６】

また、専用に規定した処理を定義したことにより、その記述が効率よく行えるとともに、暗号処理記述を実現する暗号処理装置も効率よく構成できる。そして、データを伝送する場合、暗号化鍵とともに暗号処理記述情報をともに送ることにより、伝送されるデータに特別に作り込んだ暗号復号装置を作ることなく多様なディジタルデータの暗号伝送を効率的な装置構成で実現することが出来る。

【００５７】

また、各ディジタルフォーマットに対応した暗号処理記述情報をそれぞれ用意しておき、各ファイルは、その属性に応じて対応する暗号処理記述情報に関連付けることにより、個々に暗号化記述情報を管理する必要がなく、効率的な記録管

理が行える。また、各記録メディア毎に暗号記述情報により暗号化処理を規定しておき、データを移動する場合に、その記録メディアに適した暗号化処理に変換できるために、ランダムアクセス性などを失うことなく暗号データ記録が行える。

【００５８】

なお本実施の形態では、図２のように規定した特定の命令の規定に基づいて、たとえば、図３のようなプログラム記述を暗号処理記述情報としたが、それ以外でも、たとえば、同期検出ヘッダーパターンとフレーム長検出のためのパラメータを並べあげたパラメータ記述的な表現を用いてもよいし、C言語のような汎用なソフトウエア記述言語を用いてもよい。また、特別に規定した処理も、ヘッダー検出やフレーム以外のものでもよい。たとえば、処理が複雑になるがヘッダーを検出してフレーム長を同時に検出処理を規定することでも出来し、逆にもう少し汎用的な定義として、指定ビット参照位置を移動して指定のビット数を読み取る命令を算術演算で表現する方法もある。また、記述されたプログラムもテキストのままでもよいし、所定の方法によりバイナリーコードへ変換して効率的に送ることも考えられる。

【００５９】

また、本実施の形態では、入力データ解析手段としてヘッダー検出部、フレーム長検出部を持っているが、特にそれだけに限定しているものではない。たとえば、暗号処理記述データの専用命令関数が単なる参照位置移動とデータ読み出しなどで記述されるときなどの時では、単にビットシフト部やデータ読み出し部などの単純な処理のものであってもよい。また、入力解析処理手段が入力データのみを見て動作しているものを実施例で示したが、たとえば動的に外部からフレーム長を受け取る場合など考えられる。これらについても暗号処理記述データとして外部からのパラメータ制御を規定し、入力解析手段として外部入力手段を処理部に持たせることでこれを行うことが出来る。

【００６０】

また、本実施の形態における暗号伝送装置おける伝送方法についても暗号化鍵に加えて暗号処理記述情報が復号側に送られる構成であれば、さまざまな伝送方

法が考えられ特に本実施の形態の伝送方法に限定するものではない。

【００６１】

また、本実施の形態においては、各データについて、そのフォーマット属性毎に暗号処理記述情報を用意してそれに各データを関連づけて管理した例を示したが、個々の独立に暗号処理記述情報を持ってもよいし、同じフォーマットでも別の暗号処理を行って別の暗号処理記述を持たせてもよい。同様に、記録メディア毎に暗号処理記述情報をもち、それにより記録データの暗号化処理を規定した例を示したがここに暗号処理記述情報を持たせて別の暗号処理を行ってもよい。

【００６２】

また、本実施の形態において、データの書き込み読み込み装置とデータ記憶装置に処理間の処理手続き例を示したが、その記録メディアの他のデータ伝送形式にあわせて伝送形態について特に限定するものでないし、最終的に書き込み時に用いた暗号化鍵と暗号処理記述情報が読み出し時に取得できて暗号復号出来ならば、別の方法でもよい。

【００６３】

また、本実施の形態における暗号処理装置および暗号復号装置の構成以外でも同等の処理をソフトウエアですべて実現し、CPU上で実行するような構成でも一つのソフトウエアで多様なデータフォーマットに対応出来き、同様の効果が実現できる。

【００６４】

また、本実施の形態では、暗号処理記述の例を図３に示したが、図2のような専用処理を組み合わせるとさまざまな処理が記述可能である。図１１は、典型的なディジタルフォーマットでの暗号処理例の説明図である。固定長フレーム中のデータ領域への暗号処理や、可変長パケットの様にその長さを検出後、暗号処理領域を確定し、暗号化処理する。一定周期毎に処理を更新する場合など、これらの処理を図２に規定に基づき記述することも可能であり、多様な暗号処理を記述するために用いることが出来る。

【００６５】

【発明の効果】

以上説明したように、本発明では、暗号処理をどの様に施すかを示す暗号処理記述情報をもとに暗号処理する暗号処理装置および暗号復号処理装置の構成により、多様なディジタルデータに対して適切な暗号処理を特にそのデータのために特別な装置を作ることなく、実現することが出来る。また、それを用いた効率的な暗号伝送装置が構成できる。また、メディア間で適切な暗号処理の付け替え変換が行える暗号変換装置、ファイル管理方法などを提供することができ、本発明の実用的効果は大きい。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態における暗号処理装置の構成図

【図２】

本発明の実施の形態における暗号処理記述情報を表現するために定義した処理命令関数の説明図

【図３】

本発明の実施の形態における図２で定義された関数を用いて記述された暗号処理記述情報の例の説明図

【図４】

本発明の第２の実施の形態である暗号復号装置の構成図

【図５】

本発明の実施の形態における暗号伝送装置の構成図

【図６】

本発明の第3の実施の形態である暗号処理装置を用いたデータ書き込み読み出し装置およびデータ記憶装置の構成図

【図７】

本発明の実施の形態におけるデータ記憶装置６０２内でのファイルの記録構成の説明図

【図８】

本発明の実施の形態におけるデータ書き込み時の制御部６０３と制御部６０７間の処理フローの説明図

【図９】

本発明の実施の形態におけるデータ読み出し時の制御部６０３および制御部６０７の処理フローの説明図

【図１０】

本発明の実施の形態における暗号処理変換処理の説明図

【図１１】

典型的なディジタルフォーマットでの暗号処理例の説明図

【符号の説明】

１０１　暗号処理装置
１０２　制御部
１０３　暗号処理部
１０４　フレーム長検出部
１０５　ヘッダー検出部
４０１　暗号処理装置
４０２　制御部
４０３　暗号復号処理部
４０４　フレーム長検出部
４０５　ヘッダー検出部
５０１　暗号処理記述情報
５０２　暗号処理装置
５０３　多重送信装置
５０４　受信多重分離装置
５０５　暗号処理記述言語
５０１　暗号処理記述情報
５０６　暗号復号処理装置
６０１　データ書き込み読み出し装置
６０２　データ記憶装置
６０３　制御部
６０４　鍵生成部

６０５　暗号／復号処理部

６０６　記録部

６０７　制御部

６０８　暗号処理記述情報記憶部

６０９　メディアID番号記憶部

６１０　データ記録部

８０１　書き込みファイル指定処理

８０２　メディアIDおよび暗号処理記述情報送出処理

８０３　暗号化鍵設定処理

８０４　暗号処理記述情報設定処理

８０５　暗号化およびデータ送出処理

８０６　受信データ記録処理

９０１　読み出しファイル名送出処理

９０２　暗号処理記述情報およびメディアID送出処理

９０３　暗号化鍵設定処理

９０４　暗号記述情報設定処理

９０５　データ送信リクエスト処理

９０６　データ送信処理

９０７　データ受信処理

１００１　記録メディア

１００２　記録メディア

１００３　メディアID読み取り部

１００４　メディアID読み取り部

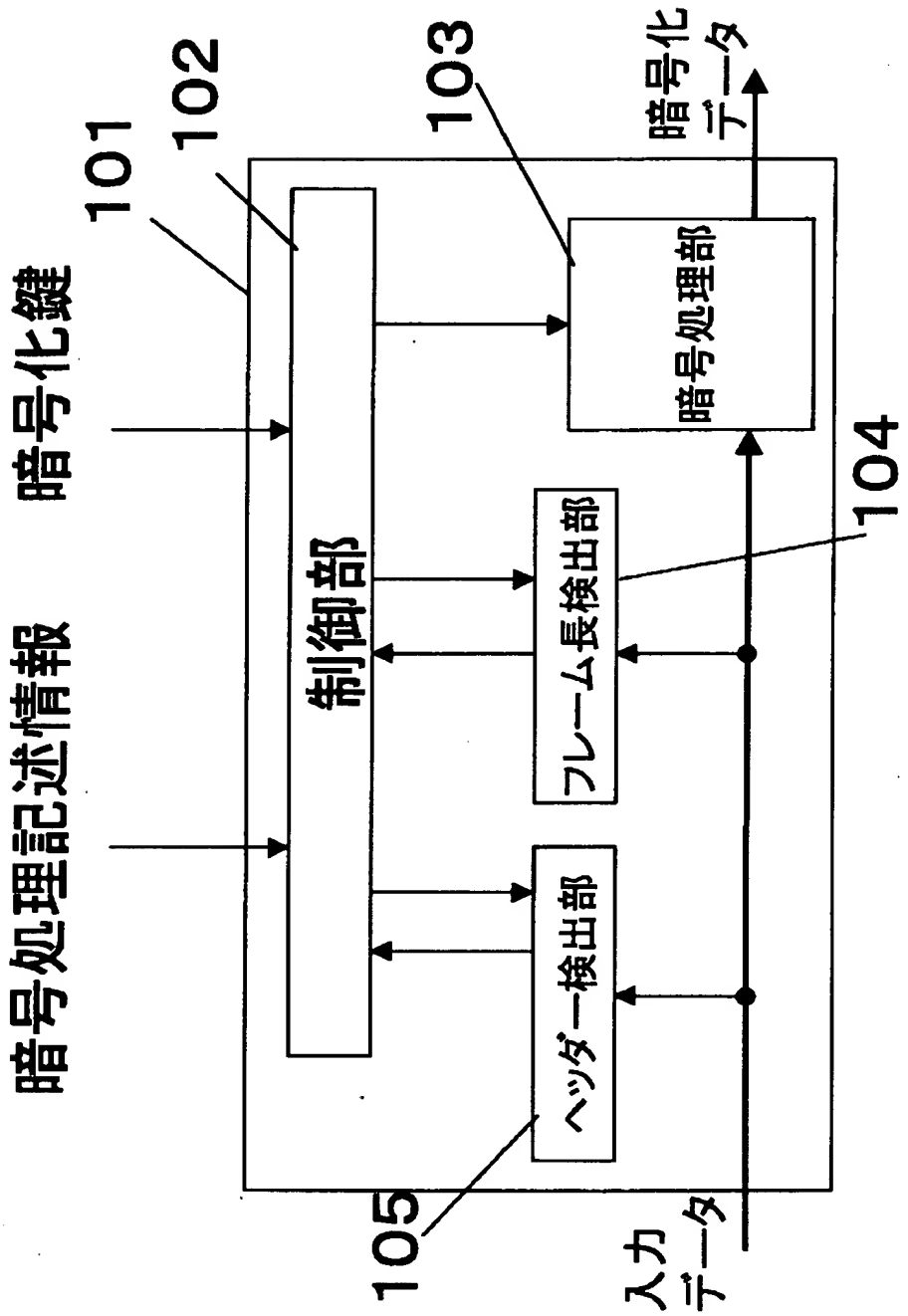
１００５　制御部

１００６　図２の暗号復号処理装置相当の暗号復号部

１００７　図１の暗号処理装置相当の暗号処理部

【書類名】　　図面

【図１】



出証特２０００－３０４１２２４

【図２】

（１）ヘッダー検出処理

head_detect(detect_pattern_size,detect_pattern,pnt_offset)

detect_pattern_size:検出ヘッダーのパターンビットサイズ

detect_pattern:検出するヘッダービットパターン

pnt_offset:検出処理の開始位置

ヘッダービットパターンをpnt_offset位置より検出を開始し、
最初のパターン検出位置へデータ参照位置reference_pntを移動する。

（２）フレーム長検出

framelength_detect(length_code_position,lengthcode_length,unit)

lengthcode_position:ヘッダー検出位置からのフレーム長コードまでの位置

lengthcode_length:フレームコード長を示すコードの長さ

unit:フレーム長コードが示す値の基本単位。ビットなら１、バイトなら８

参照位置からlengthcode_positionビットだけ移動した位置からlengthcode_lengthビット
のデータを読み出し、unit倍した値をframe_lengthとして算出。

（３）参照位置移動

reference_position_move(move_no)

move_no:移動ビット数

（４）暗号処理

encryption(algorthim_no,mode,blocklength,end_pnt)

algorthim_no:暗号アルゴリズム番号（１は、DES、２はFEALなど）

mode:適応モード（１はECB,２はOFB、３は、CBC）

blocklength:処理ブロック長

end_pnt:処理終了位置

現在の参照位置より指定の暗号処理をend_pntまで行う。処理ブロック長で
割り切れない場合は、end_pntを越えない回数行う。

出証特２０００－３０４１２２４

特平１１－１６７８９９

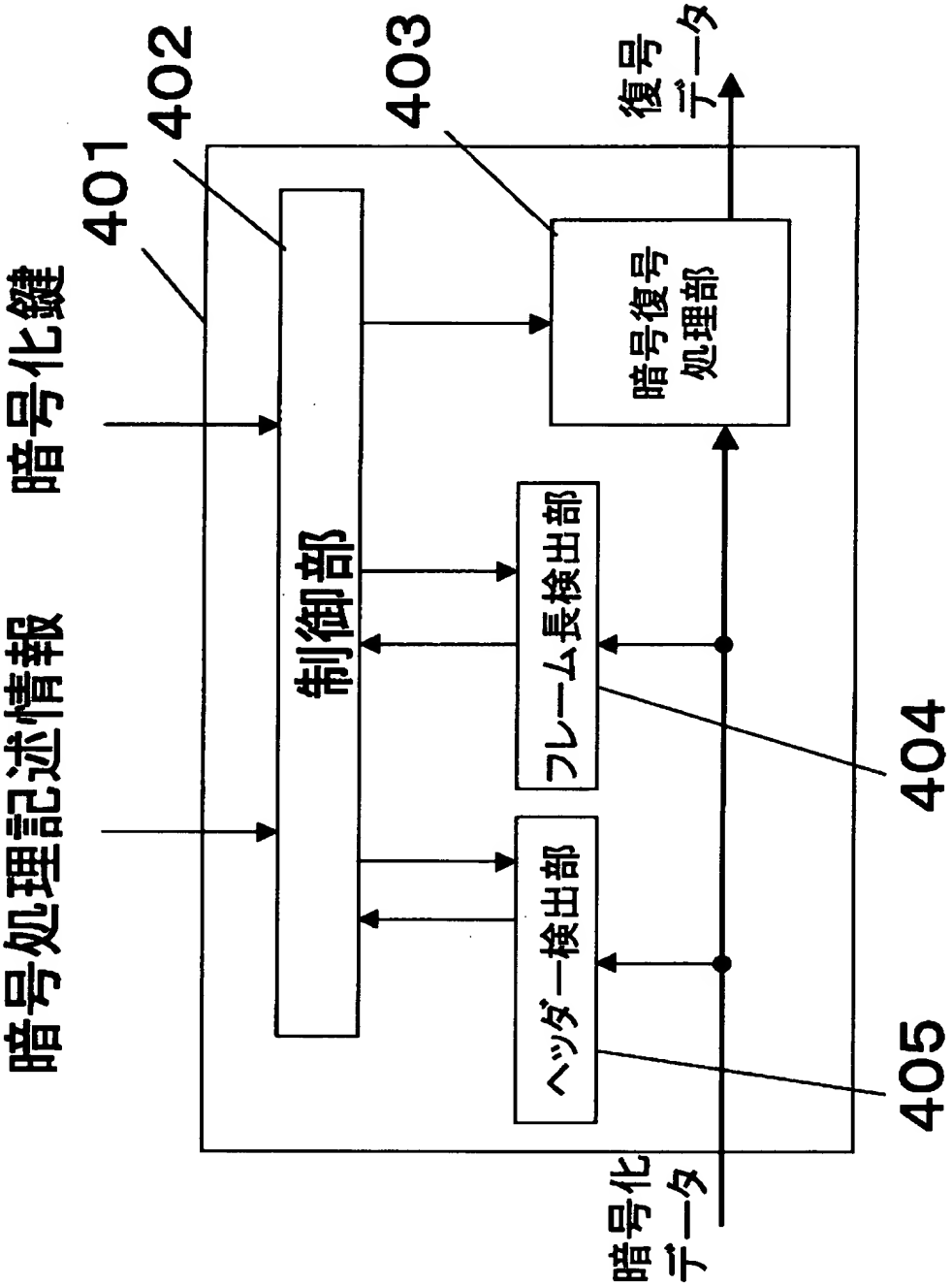
ヘッダーパターン：12ビット、16進表示FFF
フレーム長コード：ヘッダー先頭より31ビットめに13ビットでバイト単位表示
フレーム長コード以後フレーム終了までDESでCBCモード６４ビット単位で暗号化する場合

```
ref_pnt = 0;
while(endofdata)
{
        pnt_offset = ref_pnt;
        ref_pnt = head_detect(12,0xfff,ref_pnt);
        frame_length = frame_length_detect(31,13,8);
        ref_pnt  = reference_position_move(13);
        end_pnt = pnt_offset + framelength;
        encryption(1,3,64,end_pnt);
        ref_pnt = end_pnt;
}
end
```

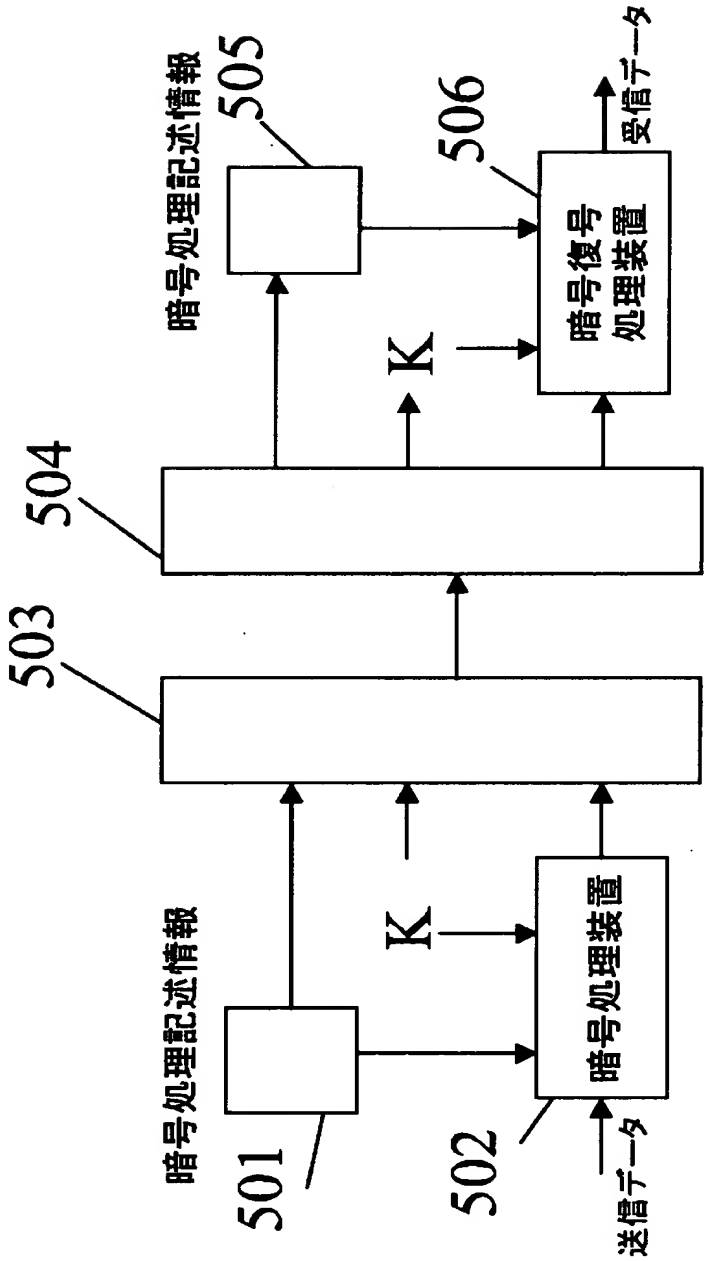

特平１１－１６７８９９

出証特２０００－３０４１２２４

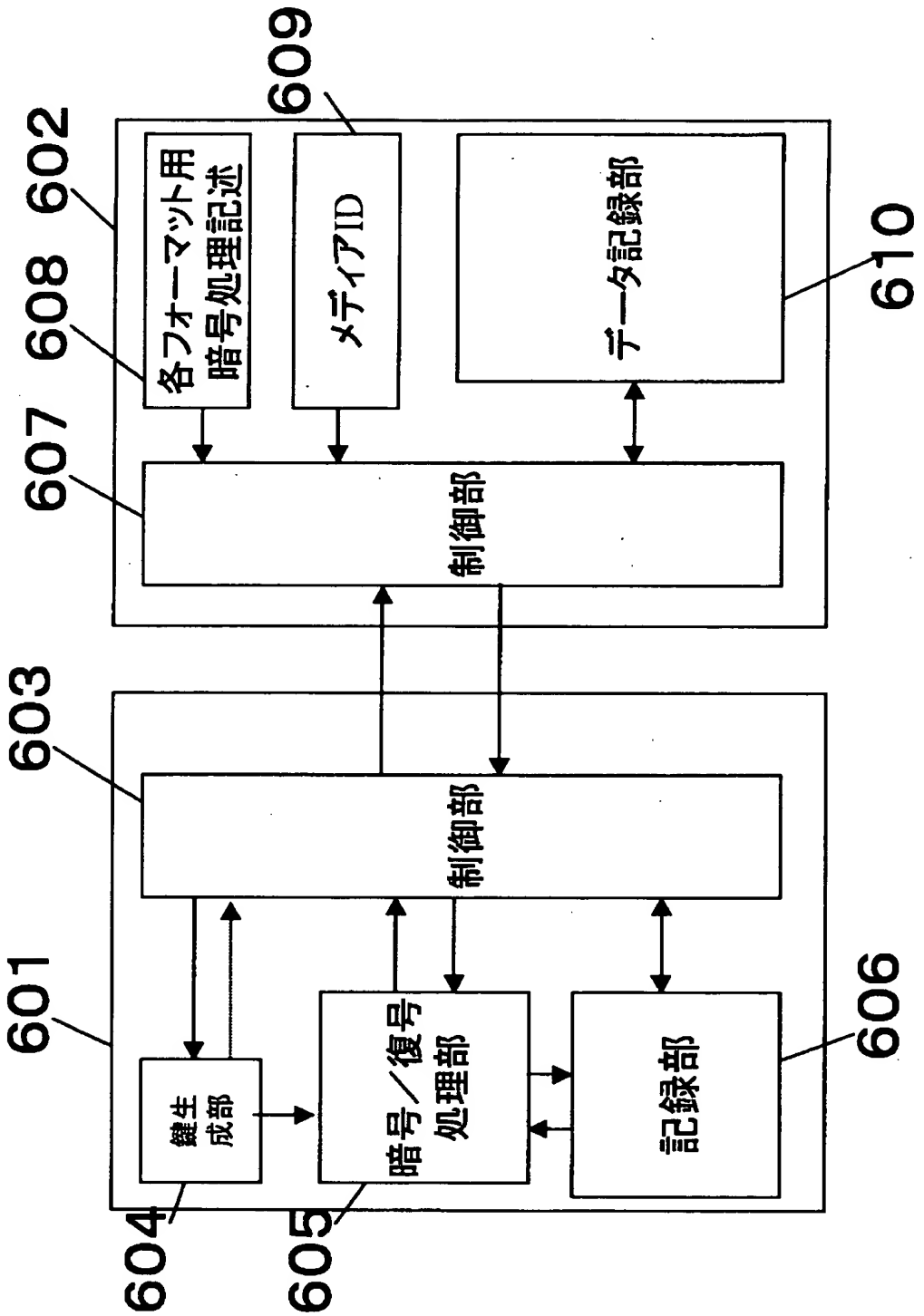
【図４】


401
402
403
404
405
暗号化鍵
暗号処理記述情報
制御部
暗号復号処理部
フレーム長検出部
ヘッダー検出部
復号データ
暗号化データ

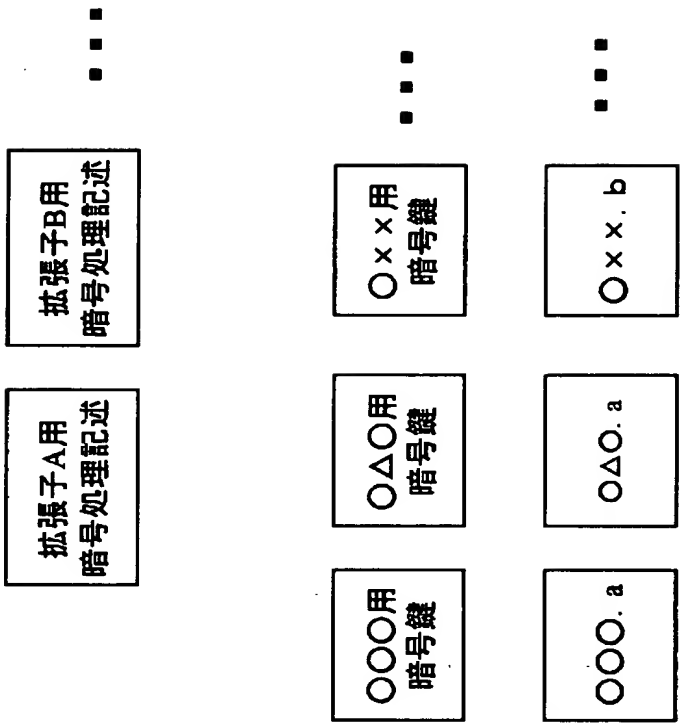
【図５】


暗号処理記述情報
505
506
受信データ
暗号復号
処理装置
K
504
503
K
暗号処理記述情報
暗号処理装置
501
502
送信データ

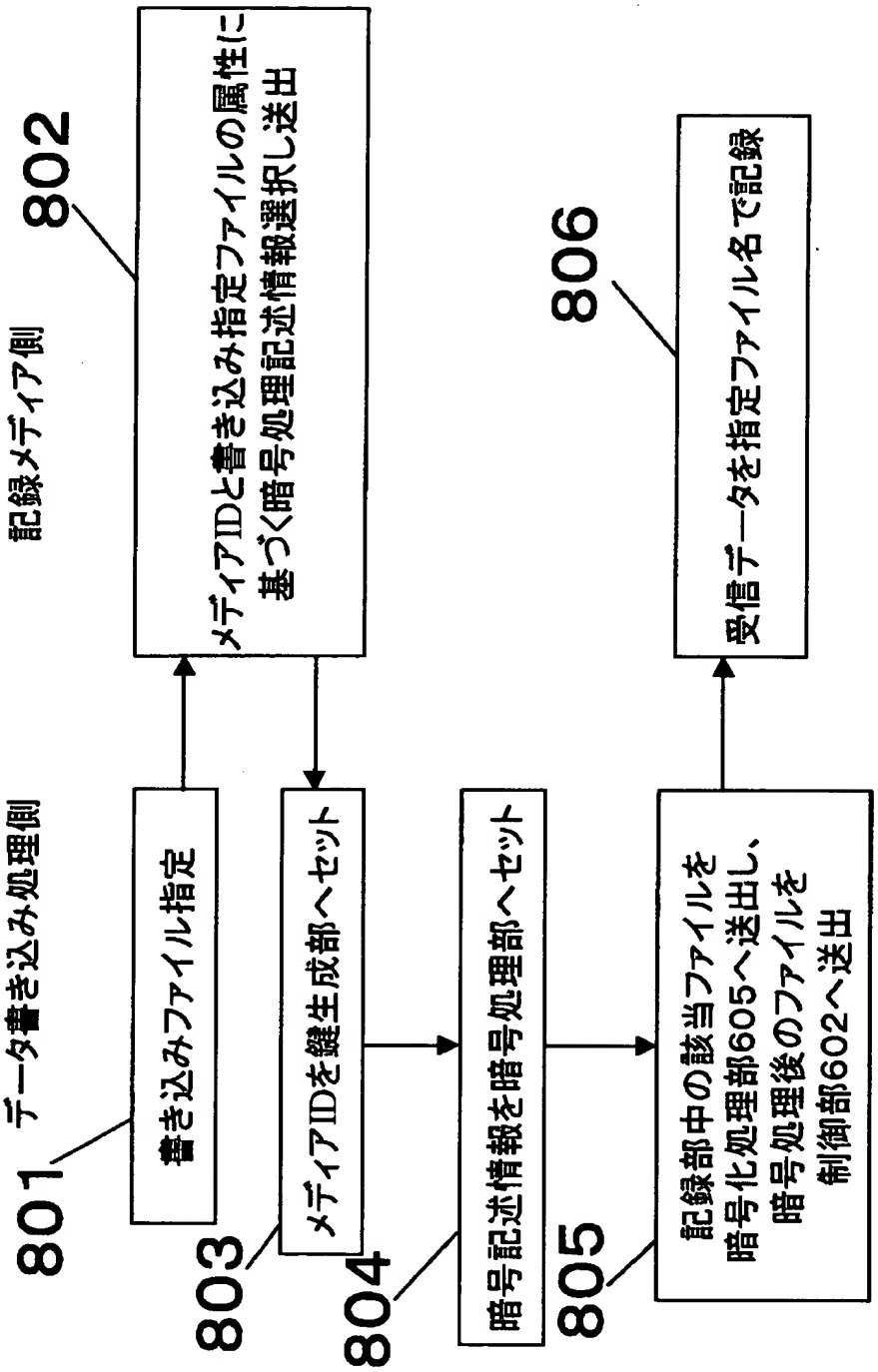
【図６】


609
602
608
607
603
601
604
605
606
610
各フォーマット用
暗号処理記述
メディアID
データ記録部
制御部
制御部
鍵生
成部
暗号／復号
処理部
記録部

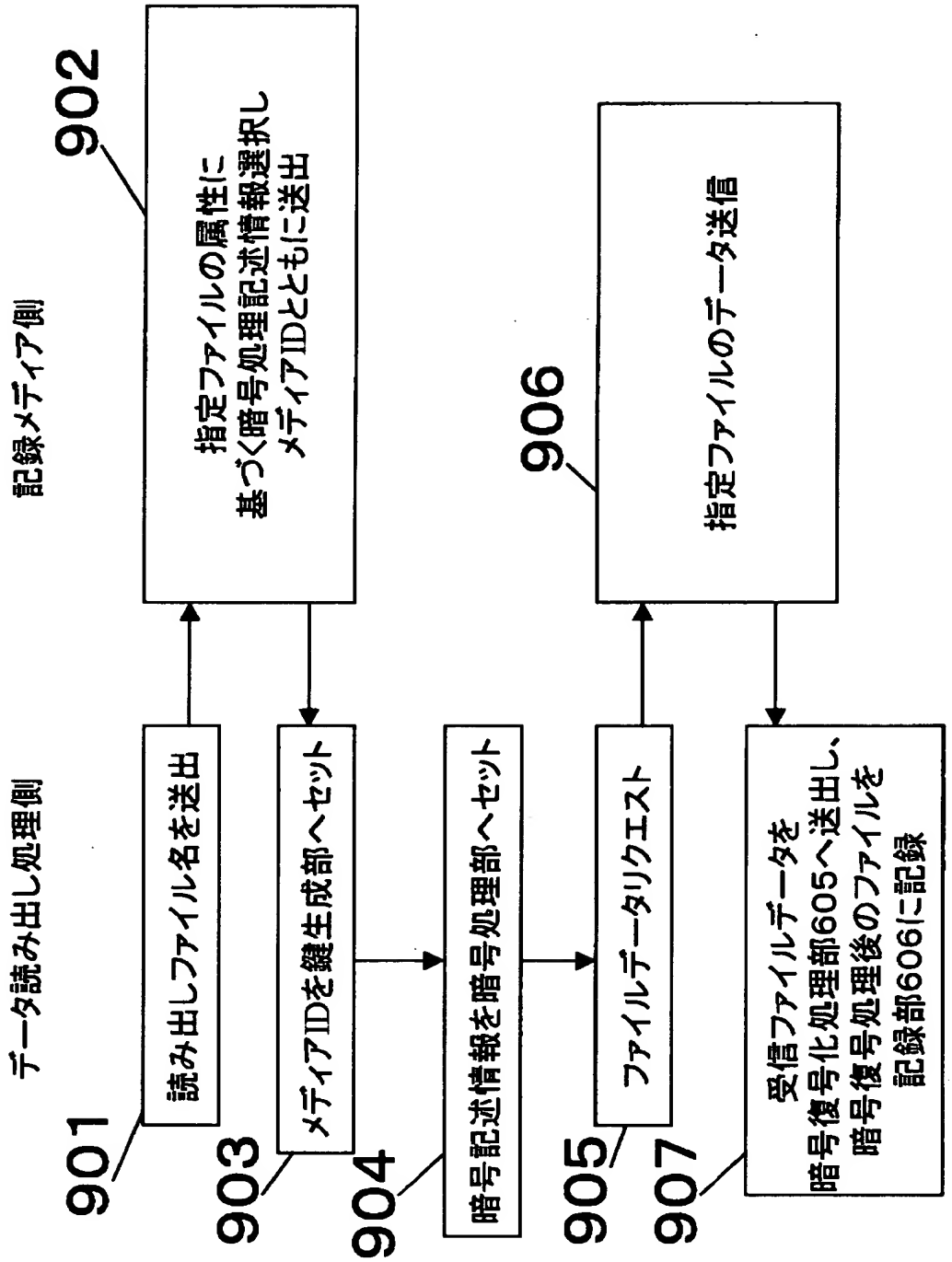
【図７】



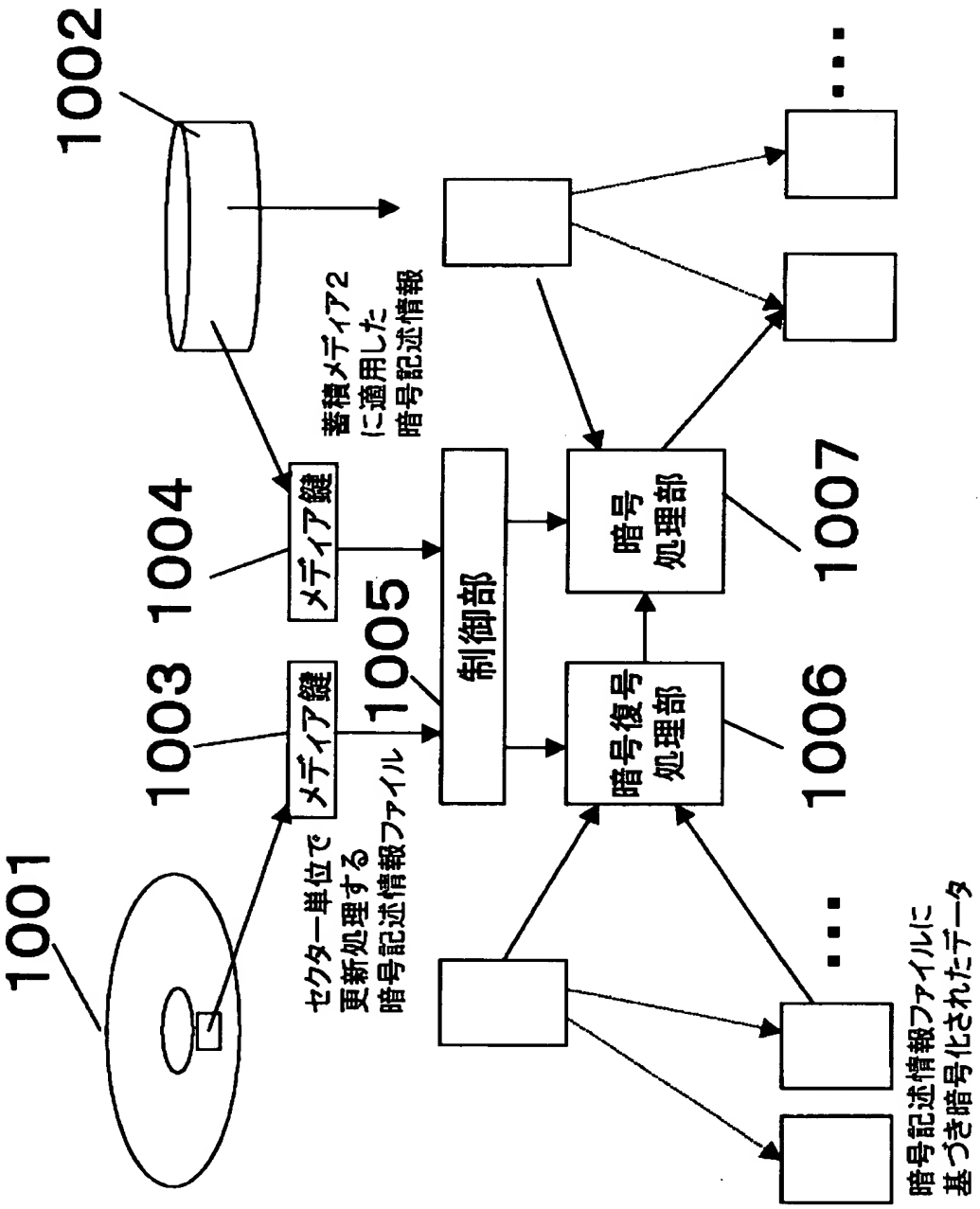
【図８】


データ書き込み処理側
記録メディア側
801
書き込みファイル指定
803
メディアIDを鍵生成部へセット
804
暗号記述情報を暗号処理部へセット
805
記録部中の該当ファイルを
暗号化処理部605へ送出し、
暗号処理後のファイルを
制御部602へ送出
806
受信データを指定ファイル名で記録
802
メディアIDと書き込み指定ファイルの属性に
基づく暗号処理記述情報選択し送出

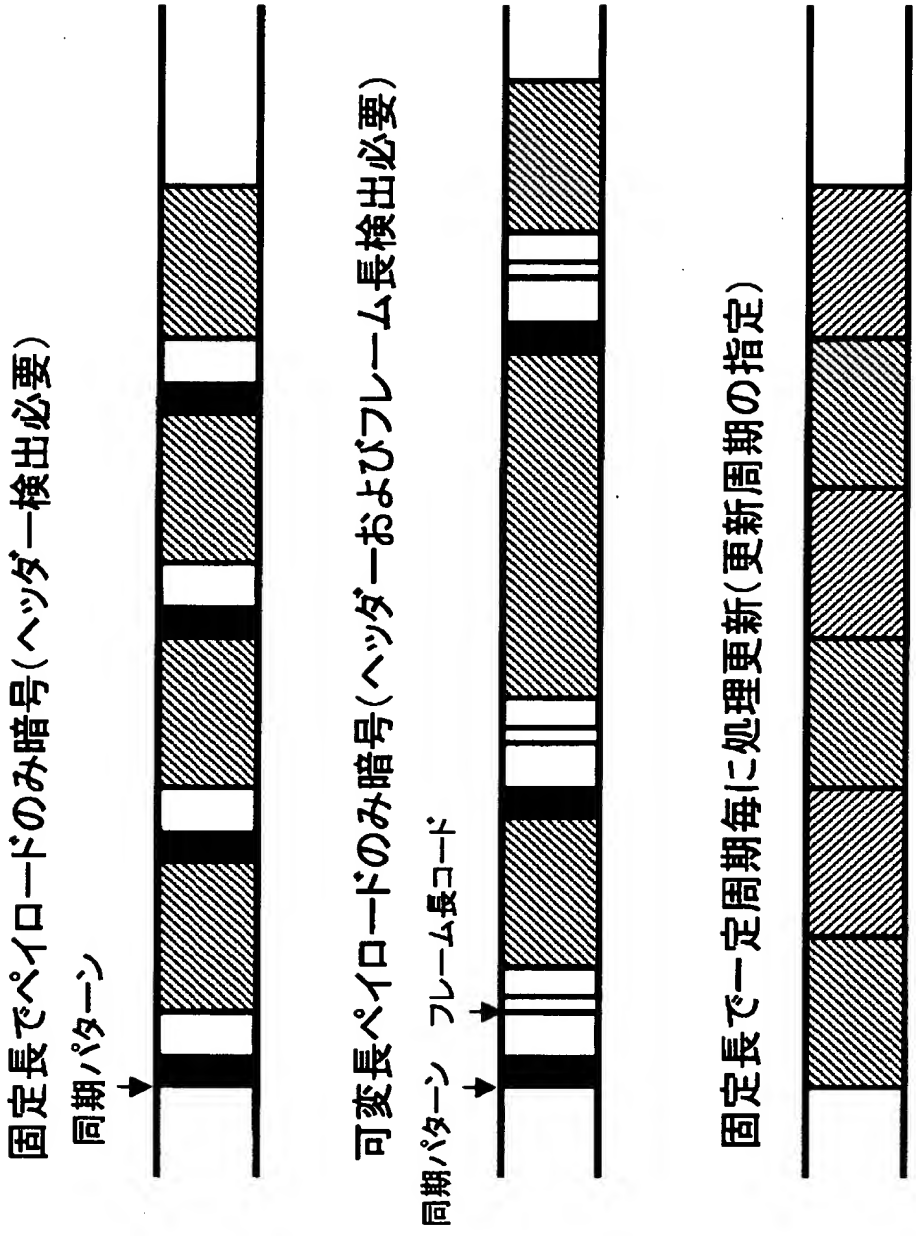
【図９】


データ読み出し処理側
記録メディア側
読み出しファイル名を送出
901
指定ファイルの属性に
基づく暗号処理記述情報選択し
メディアIDとともに送出
902
メディアIDを鍵生成部へセット
903
暗号記述情報を暗号処理部へセット
904
ファイルデータリクエスト
905
指定ファイルのデータ送信
906
受信ファイルデータを
暗号復号化処理部605へ送出し、
暗号復号処理後のファイルを
記録部606に記録
907

【図１０】


1001
1002
1003
1004
1005
1006
1007
メディア鍵
メディア鍵
制御部
暗号処理部
暗号復号処理部
蓄積メディア2に適用した暗号記述情報
セクター単位で更新処理する暗号記述情報ファイル
暗号記述情報ファイルに基づき暗号化されたデータ

【図１１】


固定長でペイロードのみ暗号（ヘッダー検出必要）
同期パターン
可変長ペイロードのみ暗号（ヘッダーおよびフレーム長検出必要）
同期パターン
フレーム長コード
固定長で一定周期毎に処理更新（更新周期の指定）

【書類名】　要約書

【要約】

【課題】　多様なディジタルデータについて、そのフォーマットに適した暗号化処理位置に暗号化処理を行う暗号化処理装置を提供することを目的とする。

【解決手段】　制御部１０２は、暗号処理記述情報に基づき、ヘッダー検出部１０５およびフレーム長検出部１０４を制御して入力データ中の暗号処理領域を求め、その暗号領域に暗号化処理するように暗号処理部１０３を制御する。入力データに応じて暗号処理記述情報を書き換えることにより、入力データに適した暗号化処理を行える。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社